David S. Casey, Jr. (SBN 60768)
Gayle M. Blatt (SBN 122048)
P. Camille Guerra (SBN 326546)
Jennifer L. Connor (SBN 241480)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
Fax: (619) 544-9232
dcasey@cglaw.com
gmb@cglaw.com
camille@cglaw.com
jconnor@cglaw.com

Attorneys for Plaintiffs, individually and on behalf of all others similarly situated

UNITED STATES DISCTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

DOBIE JAMES AUGUST, on behalf of his minor children, K.J-A. and K.D-A., individually and on behalf of all others similarly situated, Plaintiffs, vs. POWERSCHOOL HOLDINGS, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Dobie James August, on behalf of his minor children, K.J.-A and K.D.-A (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "Action") against Defendant PowerSchool Holdings, Inc. ("PowerSchool" or "Defendant"), and alleges the following:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant PowerSchool Holdings, Inc. for its failure to secure and safeguard the confidential, personally identifiable information of millions of students, parents, caregivers, school faculty and staff. The highly sensitive personal information the hackers were able to access included certain Personally Identifiable Information ("PII"), reportedly including without limitation: *e.g.*, names, home addresses, Social Security numbers, phone numbers, email addresses, grades and grade point averages, bus stops for students, passwords for student portals, notes and alerts concerning students, student IDs, in addition to other medical or protected health information ("PHI"), and also PII of parents or guardians of student (collectively, "PII/PHI").

2. Due to inadequate security, on December 28, 2024, Defendant allowed the sensitive PII/PHI of millions of individuals, the majority of which belong to students under the age of 18, to be stolen by hackers who accessed the PII/PHI through compromised login credentials and negligent security policies and practices ("Data Breach").[1] Indeed, Defendant did not have sufficient security policies or practices in place to detect or stop this Data Breach from occurring.

3. The Data Breach occurred because PowerSchool failed to implement reasonable security procedures and practices, failed to provide its employees with appropriate cybersecurity training designed to prevent and respond to data breaches, failed to take adequate steps to monitor for and detect unusual activity on its servers, and failed to disclose material facts surrounding its deficient data security protocols. In addition to violating its specific representations to consumers and the public, Defendant's actions constitute a clear failure to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII/PHI were safeguarded, failing to take available steps

[1] Cybersecurity attackers claimed in their extortion demand that they stole sensitive data from 62,488,628 students and 9,506,624 teachers. *See, https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/* (last accessed January 29, 2025).

to prevent unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

II. PARTIES

4. Plaintiff Dobie James August is the father and legal guardian of Plaintiff K.J.-A and K.D.-A. At all relevant times, he has been a resident of California. His sons attend Thurgood Marshall Middle School, which is part of the San Diego Unified District that uses PowerSchool products and services. As a result, he provided his own and his sons' PII/PHI to PowerSchool. On or about January 07, 2025, Plaintiff Dobie James August received a breach notice email from W. Drew Rowlands, the Deputy Superintendent of Operations for San Diego Unified School District notifying him that his and his sons' PII/PHI was accessed in the Data Breach.

5. Plaintiff K.J.-A is a minor under the age of 18. At all relevant times, he has been a resident of California. He attends Thurgood Marshall Middle School, which is part of the San Diego Unified School District. His school uses PowerSchool products and services. As a result, his PII/PHI was collected by PowerSchool and then subject to unauthorized access in the Data Breach.

6. Plaintiff K.D.-A is a minor under the age of 18. At all relevant times, he has been a resident of California. He attends Thurgood Marshall Middle School, which is part of the San Diego Unified School District. His school uses PowerSchool products and services. As a result, his PII/PHI was collected by PowerSchool and then subject to unauthorized access in the Data Breach.

7. Defendant PowerSchool Holdings, Inc. is a Delaware corporation with its principal place of business at 150 Parkshore Drive, Folsom, California 95630.

III. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of states different from that of at least one Class Member. The Court also has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because

Plaintiffs assert claims that necessarily raise substantial disputed federal issues under the Federal Trade Commission Act (15 U.S.C. § 45), Computer Fraud and Abuse Act (18 U.S.C. § 1030), and Stored Communications Act (18 U.S.C. § 2702). *See, e.g. infra* at ¶¶ 27-34, 90-104. This Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

9. This Court has personal jurisdiction over Defendant because, at all times relevant, Defendant is registered to do business in California with the California Secretary of State, and with its principal place of business located within California. Further, Defendant operates and is headquartered in this District and intentionally avails itself of markets within this District to render the exercise of jurisdiction by this Court just and proper.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is headquartered in this District, significant events giving rise to this case took place in this District, and because Defendant is authorized to conduct business in this District, has intentionally availed itself of the laws and markets within this District, does substantial business in this District, and is subject to personal jurisdiction in this District.

IV. FACTUAL BACKGROUND

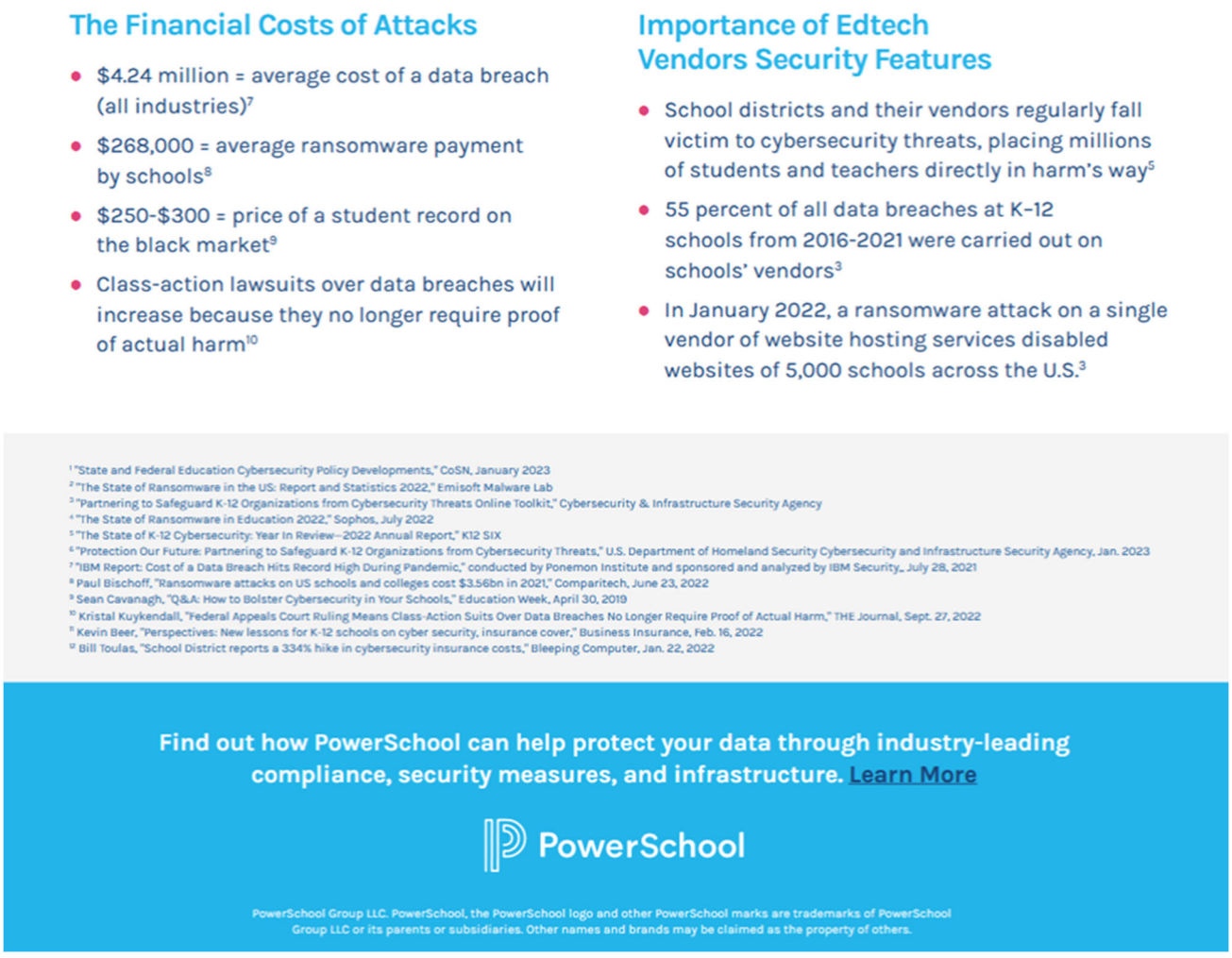
A. The PowerSchool Data Breach

11. PowerSchool is a pioneer and the leading provider of cloud-based software to the K-12 education market, providing a comprehensive platform of cloud solutions that delivers a broad range of mission-critical capabilities to K-12 organizations, including the core system of record used by districts and schools, student and teacher assessment tools, learning management systems, teacher hiring and retention solutions, and insights and analytics that leverage rich data to improve education outcomes.

12. According to its SEC Form 10-K filing for December 31, 2022, PowerSchool reports that: "We serve more than 15,000 customers, including over 90 of the 100 top districts by student enrollment in the United States, over 30 state-, province-, or territory-wide contracts in North America, and sell solutions in over 90 countries globally. Our solution is embedded in school workflows and is

used on a daily basis by teachers, students, administrators and parents in schools and districts representing over 50 million students globally, over 80% of all K-12 students in the U.S. and Canada."[2]

13. Further, PowerSchool affirmatively represents and ensures the privacy and security of the PII/PHI data it receives: Cybersecurity, Data Privacy, & Infrastructure – "PowerSchool is committed to being a good custodian of student data, taking all reasonable and appropriate countermeasures to ensure data confidentiality, integrity, and availability."[3] Moreover, PowerSchool was well-aware of the threats of cybersecurity attacks and, for example, in 2023 it presented a slideshow, noting that 45 school districts were subject to ransomware attacks the prior year, and citing K-12 cybersecurity statistical data as follows:



[2] PowerSchool Holdings, Inc., SEC Form 10-K filing for fiscal year ending December 31, 2022.

[3] https://www.powerschool.com/security/ (last accessed January 31, 2025).

At the bottom of its presentation, the slides reiterate and reassure viewers of the strength of Defendant's cybersecurity resources: "Find out how PowerSchool can help protect your data through industry-leading compliance, security measures, and infrastructure."[4] But on December 28, 2024, PowerSchool's proverbial "industry-leading compliance, security measures, and infrastructure" failed.

14. In an announcement posted on PowerSchool's website, for which there exists a separate webpage dedicated to updating information about the Data Breach, PowerSchool explains:

> ## General FAQ
>
> **What happened?**
>
> On December 28, 2024, we became aware of a potential cybersecurity incident involving unauthorized access to certain PowerSchool SIS [Student Information System ("SIS")] information through one of our community-focused customer portals, PowerSource. PowerSchool is not experiencing, nor does it expect to experience, any operational disruption and continues to provide services as normal to our customers. We have no evidence that other PowerSchool products were affected as a result of this incident or that there is any malware or continued unauthorized activity in the PowerSchool environment.
>
> * * *
>
> **FAQ for Families**
>
> * * *
>
> **Was any student or family data involved in this incident?**
>
> For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base…
>
> **FAQ for Educators**
>
> * * *

[4] https://go.powerschool.com/rs/861-RMI-846/images/K-12_Cybersecurity_Statistics.pdf

Was any educator data involved in this incident?

For involved students and educators, the types of information exfiltrated in the incident may have included one or more of the following: the individual's name, contact information, date of birth, limited medical alert information, Social Insurance Number (SIN), and other related information. Due to differences in customer requirements, the information exfiltrated for any given individual varied across our customer base…[5]

15. Despite discovering the breach on or about December 28, 2024, PowerSchool did not notify affected school districts, including San Diego Unified School District until January 7, 2025 (the "Announcement").[6] Thereafter, San Diego Unified School District then forwarded to students, parents, guardians, faculty and staff, including Plaintiffs. Moreover, Defendant failed to provide additional specific information, including the number of affected individuals or the specific type of information exfiltrated.

16. In response to the Data Breach, Defendant engaged third-party cybersecurity experts, including CrowdStrike, to investigate and mitigate the incident. After investigating the incident, it was reported that the threat actor gained access to Defendant's PowerSource portal using compromised credentials and stole data using an "export data manager" customer support tool. PowerSource contains a maintenance access tool that allows PowerSchool engineers to access Customer SIS instances for ongoing support and to troubleshoot performance issues. Using this tool, the attacker(s) exported the PowerSchool SIS 'Students' and 'Teachers' database tables to a CSV file, which was then stolen.[7]

---

[5] https://www.powerschool.com/security/sis-incident/ (last accessed January 29, 2025).

[6] Upon information and belief, at least one such Announcement reads: "As a main point of contact for your school district, we are reaching out to make you aware that on December 28, 2024 PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource." *See,* https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last accessed January 29, 2025).

[7] https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last accessed January 29, 2025)

17. Although Defendant states that the incident only impacted a subset of customers, a threat actor purportedly claimed in an extortion demand that it stole data of 62,488,628 students and 9,506,624 teachers.[8] Upon information and belief, the Data Breach involved a data-theft extortion, for which Defendant purportedly paid an undisclosed ransom amount, as opposed to a traditional ransomware attack involving encryption.[9]

18. Nearly one month after the incident, on January 27, 2025, PowerSchool began the process of filing regulatory notifications with Attorneys General Offices across applicable U.S. jurisdictions. As of the date of this filing, that regulatory breach notification process is ongoing, and individualized notifications from Defendant directed to specific students, families, faculty, and staff, including Plaintiffs - as opposed to generalized notifications *en masse* from Defendant's clients - has yet to occur. Absent detailed and individually tailored notification from Defendant, individuals are left to speculate as to which elements of their respective PII/PHI have been compromised and are without clear instruction on what they can do to protect themselves now that their PII/PHI has been exposed.

19. Personal identifying information is a valuable commodity for which a black market exists. Personal data can be worth from $1,000-$1,200 on the Dark Web,[10] [11] and the legitimate data brokerage industry is valued at more than $250 billion. Thus, Plaintiffs' and Class Members' PII/PHI has a distinct, high value – which is why legitimate companies and criminals seek to obtain and sell it.

B. Defendant Violated Its Obligations to Plaintiffs and Class Members

20. The Data Breach exposed Defendant PowerSchool's inadequate cybersecurity and privacy practices as woefully insufficient. The fact that Defendant only publicly announced the Data

---

[8] https://www.bleepingcomputer.com/news/security/powerschool-hacker-claims-they-stole-data-of-62-million-students/ (last accessed January 29, 2025)

[9] https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last accessed January 29, 2025)

[10] *See The sad truth about how much your Facebook data is worth on the dark web*, *Marketwatch*, (https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20) (Last visited 12/18/2024).

[11] *See Revealed – how much is personal information worth on the dark web?, Insurance Business Magazine*, (Last visited 12/19/2024).

Breach days after the hackers communicated that they had the stolen PII/PHI suggests that PowerSchool only "learned" of the Data Breach after the fact, as part of the hacker's extortion efforts, and not contemporaneously with any security alerts or detectors on Defendant's systems.

21. Defendant PowerSchool is a leading provider of student information systems and an array of other tools for K-12 education in the US. As promoted on its website: "Every K-12 school and district needs a quality, comprehensive student information system (SIS) at the heart of its digital ecosystem to manage educational operations. Student information systems handle a wide range of administrative functions, including collecting, storing, and providing access to student data." Also, described in its SEC filing, PowerSchool lists as one competitive strength: "Unique Data Asset, Analytics and Insight. Our leading SIS is the most comprehensive system of record for student data—enrollment, grades, attendance, health, behavior, transcripts, report cards and student fees."[12]

22. Given that the nature of PowerSchool's business involves collecting and storing highly sensitive PII/PHI for millions of students, families and guardians, faculty and staff, Defendant had a duty to secure and safeguard the information entrusted to it.

23. At all relevant times, PowerSchool had a non-delegable duty to Plaintiffs and Class Members to properly secure their PII/PHI, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Defendant became aware that their PII/PHI may have been compromised.

24. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members relied on Defendant to secure their PHI and PII when they entrusted Defendant with their sensitive and other information required to obtain Defendant's services.

[12] PowerSchool Holdings, Inc., SEC Form 10-K filing for fiscal year ending December 31, 2022.

25. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in adequate security measures, despite its obligation to protect PII/PHI. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

26. As a direct result of Defendant's failure to secure and safeguard the sensitive information of individuals that entrusted them to do so, all of this sensitive PII/PHI is in the hands of cybercriminals.

C. Defendant Failed to Comply with FTC Guidelines

27. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

28. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines provide that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[13]

29. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

30. The FTC further recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[13] *See Protecting Personal Information: A Guide for Business, Federal Trade Commission* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, (Last visited 12/17/2024).

[14] *Id.*

31. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

32. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect personal identifying information, including such PII/PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

33. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII/PHI or to comply with applicable industry standards constitutes and unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

34. Defendant was at all times fully aware of its obligation to protect the PII/PHI of its customers; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

D. Plaintiffs and Class Members Suffered Cognizable Injuries

35. Plaintiffs provided directly to Defendant, or vis-à-vis Defendant's clients, certain PII/PHI pertaining to him and his two sons, Plaintiffs K.J.-A and K.D.-A, as a condition to their enrollment and receiving educational services from Thurgood Marshall Middle School, part of the San Diego Unified School District. At the time of the Data Breach, Defendant retained Plaintiffs' sensitive PII/PHI in its systems.

36. Upon information and belief, Plaintiffs' PII/PHI was compromised in the Data Breach and stolen by hackers who illegally accessed Defendant's network for the specific purpose of targeting said PII/PHI.

37. Plaintiffs and Class Members have been damaged by the compromise of their PII/PHI in the Data Breach. The PII/PHI of consumers, such as Plaintiffs and Class Members, is valuable and has been commoditized in recent years.

38. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII/PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

39. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

40. Stolen PII/PHI is often trafficked on the "Dark Web." A heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "Dark Web" due to this encryption, which allows users and criminals to conceal identities and online activity.

41. Plaintiffs and Class Members suffered a loss of value of their PII/PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

42. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

43. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs' and other Class Members' PII/PHI, Plaintiffs and the other Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia,* (i) the untimely and inadequate notification of the Data Breach, ii) the resulting immediate increased risk of future ascertainable losses, economic damages, and other actual injury and harm, iii) the opportunity

cost and value of lost time they must spend to monitor their financial accounts and other accounts – for which they are entitled to compensation; iv) out-of-pocket expenses for securing identify theft protection and other similar necessary service.

44. Plaintiffs and Class Members also suffered a loss of value of their PHI/PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

45. Moreover, because the Data Breach involved PII/PHI pertaining to minors under the age of 18, there are additional concerns. For example, according to law enforcement professional Robert P. Chappell, Jr., a child's information can be stolen at birth and used until the child turns eighteen years old before the child realizes they've been victimized.[15]

46. The risk to Plaintiff Dobie James August's children, K.J.-A and K.D.-A, as minors, is substantial given their lack of established credit because the information can be used to create a "clean identity slate."

47. As a result of the Data Breach, Plaintiffs anticipate that they and Class Members will spend considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiffs and Class Members will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of their lives.

V. CLASS ALLEGATIONS

48. Plaintiffs bring this class action pursuant to Fed. Rules of Civ. Procedure, Rule 23(b)(2), 23(b)(3), and 23(c)(4), on behalf of themselves and all others similarly situated, as a member of a proposed nationwide class defined as follows:

> **Nationwide Class:** All United States residents whose PII/PHI was compromised in the Data Breach involving PowerSchool that occurred on or around December 28, 2024 (collectively, "the Nationwide Class" or "Nationwide Class Members").

Excluded from the Nationwide Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely and valid election to be excluded from

[15] https://www.parents.com/kids/safety/tips/what-is-child-identity-theft/ (last accessed on May 10, 2021).

this proceeding, any and all federal, state or local governments, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

49. Plaintiffs also seek to represent a California Subclass defined as follows:

> **California Subclass:** All residents of the State of California whose PII/PHI was compromised in the Data Breach involving PowerSchool that occurred on or around December 28, 2024 (collectively, "the California Subclass" or "California Subclass Members").

Collectively, the Nationwide Class and California Subclass will be referred to as "the Class" and "Class Members" unless there is a need to differentiate them.

50. In the alternative, Plaintiffs request additional classes and/or subclasses as necessary based on the types of PII/PHI that were compromised and/or subsets of individuals impacted.

51. This action has been brought and may be maintained as a class action because there is a well-defined community of interest in the litigation and the proposed Class/Subclasses are ascertainable, as described below.

52. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is at least over one million individuals. Membership in the Class may be determined by various means, including by analysis of Defendant's records).

53. Commonality: Plaintiffs and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

i. Whether Defendant had a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII/PHI;

ii. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

iii. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

iv. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

v. Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

vi. Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their PII/PHI had been compromised;

vii. How and when Defendant actually learned of the Data Breach;

viii. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII/PHI of Plaintiffs and Class Members;

ix. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

x. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII/PHI;

xi. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

xii. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

54. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

55. Adequacy of Representation: Plaintiff Dobie James August is an adequate representative of the Class in that Plaintiff has the same interests in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who is experienced in conducting litigation of this nature. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entirety. Plaintiffs do not anticipate management difficulties in this litigation.

56. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to the enormous expense of individual litigation. This makes it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

57. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

58. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct concerning the Class in its entirety, not on facts or law applicable only to Plaintiffs.

CAUSES OF ACTION

COUNT ONE

(Negligence)

(On Behalf of Plaintiffs and the Nationwide Class)

59. Each and every allegation of the preceding paragraph is incorporated in this Count with the same force and effect as though fully set forth herein.

60. Upon gaining access to the PII/PHI of Plaintiffs and Class Members, Defendant owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, update and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII/PHI of Plaintiffs and the Class. Defendant further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

61. Defendant owed this duty to Plaintiffs and Class Members because Plaintiffs and Class Members compose a well-defined, foreseeable, and probable class of individuals, including a number of vulnerable minors under the age of 18, whom Defendant was and should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited K-12 school districts, and other public, private, and charter school clients – organizations who collectively represent 80% of the K-12 students in the United States and Canada - who entrusted Defendant with Plaintiffs' and Class Members' PII/PHI. To facilitate these services, Defendant used, handled, gathered, and stored the PII/PHI of Plaintiffs and the other Class Members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII/PHI that Defendant actively solicited from clients. As such, Defendant knew a breach of its systems would cause damage to its clients and Plaintiffs and the other Class Members. Thus, Defendant had a duty to act reasonably in protecting the PII/PHI of their clients.

62. Defendant also owed a duty to timely and accurately disclose to its clients and those impacted students, families, guardians, faculty, and staff, including Plaintiffs, and Class Members, the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and other Class Members can take appropriate measures to avoid unauthorized use of their PII/PHI, accounts, cancel, and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps to mitigate the harm cause by the Data Breach and Defendant's unreasonable misconduct.

63. Defendant breached its duty to Plaintiff and other Class Members by failing to implement and maintain security controls that were capable of adequately protecting the PII/PHI of Plaintiffs and Class Members.

64. Defendant also breached its duty to timely and accurately disclose to the clients, Plaintiffs and the Class Members that their PII/PHI had been or was reasonably believed to have been improperly accessed or stolen.

65. Defendant's negligence in failing to exercise reasonable care in protecting the PII/PHI of Plaintiffs and the Class Members if further evidenced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

66. The injuries to Plaintiffs and Class Members were reasonably foreseeable to Defendant because laws and statutes, and industry standards required Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and Class Members' PII/PHI.

67. The injuries to Plaintiffs and Class Members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII/PHI were inadequately secured, non-encrypted, and exposed PII/PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiffs and Class Members.

68. As a direct proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered theft of their PII/PHI. Defendant allowed thieves access to Class Members' PII/PHI, thereby decreasing the security of Class Members' financial, social, academic, and/or health accounts, making Class Members' identities less secure and reliable, and subjecting Class Members to the imminent threat of identity theft and/or dissemination of their PII/PHI in the black markets.

69. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendant maintained belonging to Plaintiffs and Class Members; (b) violation of their privacy rights; (c) the compromise, publication, and/or theft of their PII/PHI; (d) lost money paid to Defendant and/or clients of Defendants and loss of the benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) the present, imminent and impending injury arising from the increased risk of identity theft and fraud. Not only will Plaintiffs and Class Members have to incur time and money to re-secure their accounts and identities, but they will also have to protect against identity theft for years to come - especially given the significantly large population of student minors under the age of 18.

70. As a direct and legal result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT TWO

(Violation of the California Consumer Privacy Act

Cal. Civ. Code §§ 1798.150 et seq.)

(On Behalf of Plaintiffs and the California Sub-Class)

71. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

72. Defendant violated section 1798.150(a) of the California Consumer Privacy Act by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII/PHI of Plaintiffs and the Class. As a direct and proximate

result, Plaintiffs' and the Class's PII/PHI was subject to unauthorized access and exfiltration, theft, or disclosure.

73. Defendant is a business organized for profit or financial benefit of its owners, has a gross revenue exceeding $25 million and, on information and belief, Defendant collects, receives, stores, hosts, maintains, operates, reports, and shares data, including PII/PHI, pertaining to over 19 million students in K-12 schools the United States. As a direct and proximate result of Defendant's acts, Plaintiffs and Class Members were injured and lost money, property, and/or interest in the confidentiality and privacy of their PII/PHI, and additional losses described above.

74. Plaintiffs and Class Members seek relief under California Civil Code section 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorney's fees and costs.

75. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards the PII/PHI of students, parents, legal guardians, faculty, and staff by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII/PHI, including Plaintiffs' and Class Members' PII/PHI. These individuals have an interest in ensuring that their PII/PHI is reasonably protected.

76. On January 31, 2025, Plaintiffs served on Defendant a notice letter to Defendant's registered service agent via certified mail as required by Civil Code section 1798.150(b). Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiffs believe no such cure is possible under these facts and circumstances, Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the Class as authorized by the CCPA.

COUNT THREE

(Violation of the California Unfair Competition Law,

Cal. Bus. & Prof. Code § 17200, et seq.)

(On Behalf of Plaintiffs, Nationwide Class, and the California Sub-Class)

77. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

78. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 et seq. ("UCL") prohibits any "fraudulent," or "unfair" or "unlawful" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

79. By reason of Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, as described above, and the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI Defendant engaged in unfair practices within the meaning of the UCL.

80. Defendant has violated the UCL by engaging in unfair business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in the UCL with respect to the services provided to the Class.

81. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the PII/PHI of Plaintiffs and Class Members was not maintained in accordance with Defendant's duties and responsibilities, which resulted in the compromise of massive quantities of Class Member sensitive and personal information.

82. Defendant also engaged in unfair business practices, along with unlawful practices, under the "tethering test." Defendant's actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that…all individuals have a right of privacy in information pertaining to them…The increasing use of computers…has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter

[including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

83. Defendant's wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII/PHI also constitute "unfair" business acts and practices within the meaning the UCL in that Defendant's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, oppressive and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

84. Defendant's business practices as alleged herein are wrongful and unfair because, through the specific statements described above, Defendant is likely to mislead consumers and the public into believing that the PII/PHI provided to Defendant will remain private and secure, when in fact it has not been maintained in a private and secure manner, that Defendant would employ computer systems and practices to prevent the access to and downloading of PII/PHI, when in fact it did not, and that Defendant would take proper measures to investigate and remediate a data breach as such, when Defendant did not do so.

85. Defendant's business practices as alleged herein are unlawful because, inter alia, by establishing substandard security practices and procedures and failing to take reasonable measures to protect Plaintiffs' and Class Members' PII/PHI, Defendant violated federal statutory and common laws alleged herein, including the Federal Trade Commission Act, 15 U.S.C. § 45, the Stored Communications Act ("SCA"), 18 U.S.C. § 2702 et seq., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., along with the HIPAA, 42 U.S.C. §§ 1302d, et seq., and Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 to the extent protected health information is also involved.

86. Defendant's business practices as alleged herein are also unlawful and in violation of state statutory and common laws alleged herein, including Cal. Civ. Code § 56 et seq. and Civil Code § 1798 et seq., because it failed to take reasonable measures to protect Plaintiffs' and Class Members' PII/PHI, and because it failed to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

87. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

88. Plaintiffs and Class Members have suffered and continue to suffer injury in fact and lost money or property as a direct and legal result of Defendant's unfair competition and violation of the UCL, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII/PHI, nominal damages, and additional losses as described above.

89. Plaintiffs, on behalf of the Class, seeks relief under the UCL, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of Defendant's unfair and fraudulent business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief. Plaintiffs' otherwise do not have an adequate remedy at law.

COUNT FOUR

(Computer Fraud and Abuse Act,

18 U.S.C. § 1030)

(On behalf of Plaintiffs and the Nationwide Class)

90. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

91. The Computer Fraud and Abuse Act ("CFAA") prohibits unauthorized access to protected computers and imposes liability for intentional or negligent acts that cause damage or loss. *See,* 18 U.S.C. § 1030(a)(5) and (a)(2)(C).

92. Defendant operated and maintained servers and computer systems used for storing sensitive PII/PHI for Plaintiffs and Class Members. These servers are protected computers involved in interstate commerce or communication under 18 U.S.C. § 1030(e)(2).

93. By failing to implement and maintain reasonable data security measures, Defendant allowed unauthorized third parties to access these protected computers, resulting in the theft of Plaintiffs' and Class Members' sensitive PII/PHI data.

94. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by negligently allowing unauthorized access to obtain information from a protected computer.

95. Defendant violated 18 U.S.C. § 1030(a)(5)(A)-(C) by recklessly or negligently failing to prevent unauthorized access, which caused damage and loss.

96. Plaintiffs and Class Members suffered damages exceeding the statutory threshold of $5,000 in aggregate, as required by 18 U.S.C. § 1030(g), including, costs associated with credit monitoring and identity theft protection and loss of control over sensitive PII/PHI data.

97. Under 18 U.S.C. § 1030(g), Plaintiffs and Class Members are entitled to: (i) statutory damages with a minimum aggregate loss of $5,000; (ii) injunctive relief to prevent future violations; and (iii) attorneys' fees and litigation costs.

COUNT FIVE

(Violation of the Stored Communications Act,

18 U.S.C. § 2702 *et seq*.

(On Behalf of Plaintiffs and the Nationwide Class)

98. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

99. The Stored Communications Act ("SCA") prohibits providers of electronic communication services or remote computing services from knowing divulging the contents of a communication while in electronic storage to unauthorized individuals. *See*, 18 U.S.C § 2702(a)(1) and (a)(2).

100. Defendant PowerSchool Holdings, Inc., by virtue of providing its cloud-based Student Information System, acted as a remote computing service provider by storing electronic data on behalf of schools, including Thurgood Marshall Middle School, the San Diego Unified School District, and other K-12 educational institutions, pursuant to 18 U.S.C. § 2711(2).

101. Defendant violated 18 U.S.C. § 2702(a)(1) by negligently allowing unauthorized third parties to access and exfiltrate data containing the sensitive PII/PHI of Plaintiffs and Class Members.

102. Defendant failed to implement adequate safeguards to secure the private data stored on its servers, such as encryption of sensitive PII/PHI or monitoring for unauthorized access, in violation of its obligations under the SCA.

103. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered harm, including loss of control over their sensitive information, ongoing and increased risk of identity theft, and costs associated with credit monitoring.

104. Under 18 U.S.C. § 2707(c), Plaintiffs and Class Members are entitled to: (i) statutory damages, the greater of actual damages or $1,000 per violation; (ii) punitive damages for willful or intentional violation; and attorney's fees and litigation cost.

COUNT SIX

(Unjust Enrichment)

(On Behalf of Plaintiffs and the Nationwide Class)

105. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

106. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monies that the respective K-12 school districts, private, public, charter schools and other educational institutions paid on behalf of Plaintiffs and Class Members for Defendant's services. Specifically, each school is funded through private tuition, tax revenues, government funds, or a combination thereof, which is used on behalf of the students. The Defendant was then paid by each school or education institution to store, maintain, and properly secure Plaintiffs' and Class Members' PII/PHI.

107. Accordingly, a portion of such payments for goods and services made on behalf of the Plaintiffs and Class Members, who are the intended beneficiaries of a contract between Defendant and its educational institutional clients, were to be used, in part, to pay for use of Defendant's network and the administrative costs of data management and to provide a reasonable level of data security.

108. In exchange, Plaintiffs and Class Members should have received from Defendant the benefits, goods, and services that were the subject of the transaction and also have had their PII/PHI protected with adequate data security measures.

109. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted, and through which Defendant was unjustly enriched. Defendant profited from

these transactions and used the PII/PHI of Plaintiffs and Class Members for business purposes to increase their revenues.

110. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendant increased its own profits at the expense of Plaintiffs and Class Members by using ineffective security measures, failing to encrypt the data, failing to pay money for training employees, failing to conduct audits, and failing to implement other necessary security measures. The Plaintiffs and Class Members suffered injury as a direct and proximate result of Defendant's decision to prioritize profits over the requisite security measures and training.

111. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards and by Defendant's own representations.

112. Defendant failed to secure Plaintiffs' and Class Members' PII/PHI and, therefore, did not provide full compensation for the benefits Plaintiffs and Class Members paid.

113. Defendant acquired the PII/PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

114. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII/PHI, they would not have agreed to the disclosure of said PII/PHI in exchange for Defendant's services.

115. Plaintiffs and Class Members have no adequate remedy at law.

116. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendant maintained belonging to Plaintiffs and Class Members; (b) violation of their privacy rights; (c) the compromise, publication, and/or theft of their PII/PHI; (d) lost money paid to Defendant and the lost benefit of the bargain in Defendant's failure to comply with its obligations and representations, (e) the out-of-pocket costs for detecting, preventing, mitigating the effects of the Data Breach; and (f) the present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

117. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

118. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that were overpaid on behalf of the Plaintiffs and Class Members for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. An order certifying the Nationwide Class, along with the California Subclass, and declaring that Plaintiffs are the Class Representatives and appointing Plaintiffs' counsel as Class Counsel;
2. Permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, statutory, and nominal damages in an amount to be proven at trial;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. A declaration of right and liabilities of the Parties;
7. Reasonable attorneys' fees, costs, and expenses;
8. Pre- and post-judgment interest at the maximum legal rate;
9. Distribution of any monies recovered on behalf of Class Members or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendant from retaining the benefits of their wrongful conduct; and
10. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: January 31, 2025

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP

Gayle M. Blatt

David S. Casey, Jr.
Gayle M. Blatt
P. Camille Guerra
Jennifer L. Connor

Attorneys for Plaintiffs, individually and on behalf of all others similarly situated